CLAIMS

What is claimed is:

1. A method comprising:

providing a partition on a storage device of a computer system, wherein said partition is normally invisible to an operating system of the computer system unless the partition is unlocked; and

unlocking the partition in response to an unlock request received from a software task having knowledge about a proper handshake to unlock the partition, wherein the partition is visible to the operating system when it is unlocked.

2. The method of claim 1, wherein the storage device is a hard disk drive having a disk controller.

3. The method of claim 1, wherein the unlocking of the partition is initiated by establishing a proper unlock handshake between the software task and an IDE controller for controlling the storage device.

4. The method of claim 3, wherein the software task requests a master token from the IDE controller when the computer system is first turned on and the unlock handshake between the software task and the IDE controller is established by passing the master token back to the IDE controller as a parameter.

5. The method of claim 2, wherein the software task requests a master token from the disk controller when the computer system is first turned on, said master token is used by the software task to initiate the proper handshake to unlock the partition.

6. The method of claim 1, further comprising preventing an access to the partition when the partition is unlocked unless the access is requested by a software having knowledge about a proper access handshake for accessing the partition.

7. The method of claim 6, wherein the software receives a usage token from an IDE controller when the partition is unlocked and the access handshake between the software and the IDE controller is established by passing the usage token back to the IDE controller as a parameter.

8. The method of claim 1, further comprising locking the partition in response to a lock request received from a software having knowledge about a proper handshake for locking the partition.

A3

9. The method of claim 1, further comprising providing a standard partition on the storage device, wherein said standard partition is always visible to the operating system and generally accessible to other softwares.

10. A machine-readable medium that provides instructions, which when executed by a set of processors, causes said set of processors to perform operations comprising:

receiving an open request from a software to access a secure-private partition on a hard drive of a computer system;

validating the open request received from the software; and

requesting unlocking of the secure-private partition in response to the validation of the open request received from the software.

11. The machine-readable medium of claim 10, wherein the operations further comprise requesting locking of the secure-private partition in response to a close request received from the software.

12. The machine-readable medium of claim 10, wherein the requesting of the unlocking of the secure partition further comprises:

requesting a master token from an IDE controller when the computer system is turned on;

storing the master token in a secure storage location;

retrieving the master token from the secure storage location when an access to a secure-private partition is needed; and

passing the master token as a parameter to the IDE controller.

13. The machine-readable medium of claim 10, wherein the operations further comprise requesting an access to the secure-private partition in response to an access request received from the software.

14. The machine-readable medium of claim 13, wherein the requesting of the access to the secure partition further comprises:

receiving a usage token; and

passing the usage token to the IDE controller to gain an access to the secure partition.

15. The machine-readable medium of claim 10, wherein the request from the software to access the secure-private partition is received by a privacy gatekeeper which prescreens the request to determine if the software has an authorization to access the secure-private partition.

16. A system comprising:

a storage device having a storage controller, said storage device having at least one secure-private partition, wherein said secure-private partition is selectively in one of locked and unlocked modes, wherein said secure-private partition is invisible to an operating system when it is locked and the secure-private partition is visible to the operating system when it is unlocked;

an IDE controller operatively coupled to the storage controller; and

a security/privacy software task operatively coupled to the IDE controller, wherein said IDE controller initiates an unlock request to unlock the secure-private partition in response to a valid unlock handshake established between the IDE controller and the security/privacy software task and said IDE controller initiates a lock request to lock the secure-private partition in response to a valid lock handshake established between the IDE controller and the security/privacy software task.

17. The system of claim 16, wherein the security/privacy software task requests a master token from the IDE controller when the system is turned on and sends the master token to the IDE controller as a parameter when making a request to the IDE controller to unlock the secure-private partition.

18. The system of claim 16, further comprising a requesting software and a privacy gatekeeper which acts as a gatekeeper to the security/privacy software task, wherein when the requesting software makes a request to access the secure-private partition, the privacy gatekeeper prescreens the request to determine if the requesting software has an authorization to access the secure-private partition.

19. The system of claim 18, wherein the IDE controller allows an access to said at least one secure-private partition only when a valid access handshake is established between the requesting software and the IDE controller.

20. The system of claim 19, wherein the IDE controller generates and return a usage token to the requesting software once the secure-private partition is unlocked, wherein the access handshake is established between the IDE controller and the requesting software when the IDE controller validates the usage token passed back by the requesting software.